

ORDER FOR SUPPLIES AND SERVICES				IMPORTANT: See instructions in GSAR 553.370-300-1 for distribution		PAGE 1 OF 1 PAGE(S)	
1. DATE OF ORDER 03/31/2011		2. ORDER NUMBER GST0311DS8018		3. CONTRACT NUMBER GS00Q09BGD0048		4. ACT NUMBER A2473348C	
<b>FOR GOVERNMENT USE ONLY</b>	5. ACCOUNTING CLASSIFICATION				6. FINANCE DIVISION		
	FUND 299X	ORG CODE A03VR110	B/A CODE F1	O/C CODE 25	AC	SS	VENDOR NAME
	FUNC CODE C01	C/E CODE H08	PROJ./PROS. NO.	CC-A	MDL	FI	G/L DEBT
	W/ITEM	CC-B	PRT./CRFT		AI	LC	DISCOUNT
7. TO: CONTRACTOR (Name, address and zip code) Gregory Parrington SAIC. 10260 CAMPUS POINT DR SAN DIEGO, CA 92121-1522 United States (b) (6)				8. TYPE OF ORDER B. DELIVERY		REFERENCE YOUR	
				Please furnish the following on the terms specified on both sides of the order and the attached sheets, if any, including delivery as indicated.			
				This delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above numbered contract.			
				C. MODIFICATION NO. 00 TYPE OF MODIFICATION:		AUTHORITY FOR ISSUING	
9A. EMPLOYER'S IDENTIFICATION NUMBER 953630868		9B. CHECK, IF APPROP WITHHOLD 20%		Except as provided herein, all terms and conditions of the original order, as heretofore modified, remain unchanged.			
10A. CLASSIFICATION B. Other than Small Business				10B. TYPE OF BUSINESS ORGANIZATION C. Corporation			
11. ISSUING OFFICE (Address, zip code, and telephone no.) GSA Region 3 Eileen S. Flanigan 20 North Eighth Street Philadelphia, PA 19107-3191 United States (b) (6)		12. REMITTANCE ADDRESS (MANDATORY) SAIC. PO BOX 223058 PITTSBURGH, PA 15251-2058 United States		13. SHIP TO (Consignee address, zip code and telephone no.) Craig Brugger 400 GIGLING ROAD (DMDC) SEASIDE, CA 93955-6771 United States (b) (6)			
14. PLACE OF INSPECTION AND ACCEPTANCE Craig Brugger 400 GIGLING ROAD (DMDC) SEASIDE, CA 93955-6771 United States		15. REQUISITION OFFICE (Name, symbol and telephone no.) Michael Baumann GSA Region 3 20 North 8th Street, 10th Floor Philadelphia, PA 19107-3191 United States (b) (6)					
16. F.O.B. POINT Destination		17. GOVERNMENT B/L NO.		18. DELIVERY F.O.B. POINT ON OR BEFORE 03/31/2012		19. PAYMENT/DISCOUNT TERMS NET 30 DAYS / 0.00 % 0 DAYS / 0.00 % 0 DAYS	
<p align="center"><b>20. SCHEDULE</b></p> <p>Firm Fixed Price Task Order GST0311DS8018 is hereby awarded for DMDC DCII/iRR Sustainment support for a 12-month performance period of 01 April 2011 through 31 March 2012. This task order incorporates the Performance Work Statement under ITSS Control #R3114488 and accepts the Contractor's quote submitted on 02/18/2011, as revised on 03/25/2011 for a total awarded amount of (b) (4).</p> <p>This funding is subject to the availability of funds in accordance with FAR 52.232.19 Availability of Funds for the Next Fiscal Year and under the Continuing Resolution for FY11. This funding allows contractor performance through November 15, 2011. The contractor is not authorized to incur costs in excess of this amount or beyond November 15, 2011 unless additional funding is provided via formal modification signed by the Contracting Officer.</p> <p>Funding in the amount of (b) (4) is hereby provided to fully fund FFP tasks and the CAF. Funding in the amount of (b) (4) is provided for reimbursable travel under this task order. The contractor is not authorized to incur travel costs in excess of this amount unless additional funding is provided via formal modification signed by the Contracting Officer.</p> <p>The total awarded ceiling price for the base period of performance is (b) (4).</p> <p>Additionally, this task order contains one option period to be exercised as a unilateral right of the Government with a period of performance of 01 April 2012 through 31 March 2013.</p>							
ITEM NO.	SUPPLIES OR SERVICES		QUANTITY ORDERED	UNIT	UNIT PRICE	AMOUNT	
(A)	(B)		(C)	(D)	(E)	(F)	
0001	Base Period		1	lot	(b) (4)	(b) (4)	
21. RECEIVING OFFICE (Name, symbol and telephone no.) Defense Manpower Data Center Seaside, (703) 696-7396					TOTAL From 300-A(s)		
22. SHIPPING POINT Specified in QUOTE			23. GROSS SHIP WT.		GRAND TOTAL	(b) (4)	

<b>24. MAIL INVOICE TO: (Include zip code)</b> Finance Operations and Disbursement Branch (BCEB) 299X PO Box 219434 Kansas City, MO 641219434 United States	<b>25A. FOR INQUIRIES REGARDING PAYMENT CONTACT:</b> GSA Finance Customer Support	<b>25B. TELEPHONE NO.</b> 816-926-7287
	<b>26A. NAME OF CONTRACTING/ORDERING OFFICER (Type)</b> Eileen S. Flanigan	<b>26B. TELEPHONE NO.</b> (b) (6)
	<b>26C. SIGNATURE</b> Eileen S. Flanigan 03/31/2011	
<b>GENERAL SERVICES ADMINISTRATION</b>	<b>1. PAYING OFFICE</b>	<b>GSA FORM 300 (REV. 2-93)</b>

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

---

**TABLE OF CONTENTS**

---

1.0 BACKGROUND

1.1 Description of Services

1.2 Introduction

2.0 OBJECTIVES

3.0 SCOPE OF WORK

4.0 TASK REQUIREMENTS

4.1 Task 1 – Sustainment and Operational Support of DCII & iIRR

~~4.2 Task 2 – Application Failover/COOP System Support~~

4.3 Task 3 – New DCII System Stand-up Support (Transition Phase I)

4.4 Task 4 – New DCII System Stand-up Support (Transition Phase II)

4.5 Task 5 – New iIRR System Stand-up Support (Transition Phase III)

4.6 Task 6 – Functional/Technical/Subject Matter Experts

4.7 Task 7 – Configuration Management (CM) Support

4.8 Task 8 – Quality Assurance

4.9 Task 9 – Testing Support

4.10 Task 10 – User Acceptance Testing (UAT) for iIRR

4.11 Task 11 – Information Assurance/Computer Network Defense (IA/CND)

~~4.12 Task 12 – Vulnerability Management~~

~~4.13 Task 13 – System Security Engineering (SSE) Support~~

~~4.14 Task 14 – Database Administration~~

4.15 Task 15 – Data Analysis and Cleansing

4.16 Task 16 – Customer and Field Support

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

5.0 PERIOD OF PERFORMANCE

6.0 PLACE OF PERFORMANCE

7.0 DELIVERABLES AND REPORTS

7.1 Deliverables and Reports (Appendix E)

7.1.1 Problem Reports

7.1.2 Senior Management Review (SMR) Reports (Appendix X)

7.1.3 Funding Notification

7.1.4 Quality Control Plan

7.1.5 Project Staffing Plan

7.2 Delivery, Inspection, and Acceptance Instructions

8.0 CONTRACTOR PERSONNEL

8.1 Key Personnel Requirements

8.2 Identification of Contractor Employees

8.3 Organizational Conflict of Interest

8.4 Unauthorized Disclosure

9.0 SECURITY

9.1 National Agency Check & Inquiries (NACI)

9.2 Trustworthiness Determination and Security Clearances

9.3 IT Security Compliance

9.4 Privacy Act

9.5 Protection of Personally Identifiable Information (PII)

9.6 Physical Security

9.7 Government Facility Access

9.8 Personal Identity Verification of Contractor Personnel

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

**10.0 OTHER PERFORMANCE REQUIREMENTS**

- 10.1 Orientation Briefing
- 10.2 Transition/Phase-In
- 10.3 Hours of Operation
- 10.4 Government Holidays
- 10.5 Contractor Interfaces
- 10.6 Remote Access

**11.0 TRAVEL**

**12.0 GOVERNMENT FURNISHED PROPERTY/INFORMATION**

**13.0 ADMINISTRATIVE CONSIDERATIONS**

- 13.1 Correspondence
- 13.2 Points of Contact
  - 13.2.1 Contracting Officer's Technical Representative (COTR)
  - 13.2.2 Contracting Officer
  - 13.2.3 Contract Specialist
  - 13.2.4 Client Service Representative (PM/ITM)
- 13.3 Clauses

**14.0 SECTION 508 COMPLIANCE REQUIREMENTS**

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

## **1.0 BACKGROUND**

On January 15, 2009, the Deputy Secretary of Defense directed that the Department strengthen and refocus Defense Security Services to meet 21<sup>st</sup> century industrial security and counterintelligence needs. Pursuant to this recommendation, DSS was directed to transfer “DoD enterprise wide IT systems associated with personnel security clearances to the Defense Manpower Data Center.” A Memorandum of Agreement between DSS and DMDC was signed on February 2, 2010, which sets forth the terms and conditions for the transfer. The agreement also established a six-month transition period for the Information Systems. Systems affected by the transfer are the Defense Central Index of Investigations (DCII); the Joint Personnel Adjudication System (JPAS); the Investigative Records Repository (IRR) (also referred to as the “Improved Investigative Records Repository (*iIRR*); and the Secure Web Fingerprint Transmission (SWFT).

The DCII, JPAS, *iIRR*, and SWFT systems are collectively identified as the Personnel Security and Assurance (PSA) systems.

The Defense Central Index of Investigations (DCII) is an automated central index that identifies investigations conducted by Department of Defense investigative agencies. DCII is operated and maintained on behalf of the DoD components and office of the Deputy Under Secretary of Defense for HUMINT, Counterintelligence and Security. DCII access is limited to the Department of Defense and other federal agencies that have adjudicative, investigative and/or counterintelligence missions.

The improved Investigative Records Repository (*iIRR*) is a modern Information Technology (IT) system based on the application of industry best practices, and is compliant with the Enterprise Security System (ESS) architectural practices. It provides its user community access to and retrieval of legacy investigative records in a fashion that optimizes operational and cost efficiency. Legacy investigative records are defined as the subject records of any personnel security investigation within the Case Control Management System – Information System (CCMS-IS) prior to decommissioning on 3 FEB 2006. The *iIRR* system is maintained by the Defense Manpower Data Center, which is responsible for delivering the services and work products produced by the *iIRR*. The system is entirely located at a controlled facility at Iron Mountain Facility in Boyers, Pennsylvania and has no interconnections with any other systems.

During this period of performance DCII and *iIRR* will be transitioning from the DSS environments to the DMDC infrastructure. The transition will take place in three (3) phases, two for DCII and one for *iIRR*. Transition I will be transitioning DCII from the DSS enclave into DMDC enclave. Transition II will be the DCII transition from the DMDC enclave into the standard DMDC operational environment. Transition III will be the *iIRR* transition from Boyers, PA, into the standard DMDC operational environment. The contractor’s roles and

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

responsibilities will reduce after the completion of Transition II for DCII, and after Transition III for iIRR.

**1.1 Description of Services:** This is a non-personal services contract to provide software sustainment and support services to the Defense Manpower Data Center (herein after referred to as “Government”). The contractor shall be solely responsible for all supervision requirements. The Contractor, in turn, is responsible to the Government.

**1.2 Introduction:** Defense Manpower Data Center (DMDC) is part of a Department of Defense (DoD) Field Activity called the Defense Human Resources Activity (DHRA) which supports major programs and initiatives within the DoD. DMDC maintains the central and authoritative store of personnel, manpower, training, and security data for the DoD.

The personnel data holdings, in particular, are broad in scope and date back to the early 1970’s, covering all Uniformed Services, all components of the Total Force (Active, Guard, Reserve, and Civilian), and all phases of the personnel life cycle (accessions through separation/retirement). The categories of data archived at DMDC represent significant data holdings and, in most cases, provide the only single source of common data on the Uniformed Services. These data support decision-making a wide variety of organizations including the Office of the Under Secretary of Defense (Personnel and Readiness), other OSD organizations, and DMDC customers both within and outside the DoD.

DMDC operates major programs affecting individual members of the DoD, as well as other Federal Departments and Agencies. The programs support Active Duty, Reserve, Guard, and retired military members and their families, as well as civilian and contractor employees of the DoD. These programs include verifying military entitlements and benefits; managing the DoD ID card issuance program; providing identity management for the DoD; helping identify fraud and waste in DoD systems; conducting personnel surveys; performing longitudinal and statistical analyses; developing military selection, classification, and language proficiency tests; and assisting military members and their families with quality of life issues and transition to civilian life.

DMDC is a geographically separated organization with personnel and facilities located in Arlington, Virginia; Seaside, California; Boyers, Pennsylvania; Korea; Southwest Asia; and, Germany. While being geographically dispersed, DMDC takes pride in delivering timely, quality support to the DoD and its members. DMDC adds value by ensuring data received from a variety of sources is consistent, accurate, and appropriate when used to respond to inquiries. In fulfilling its mission, DMDC has successfully explored and fielded new programs, such as the Defense Language Proficiency Tests (DLPT), by leveraging existing systems and infrastructure. DMDC quickly responds to initiatives and information needs of DoD senior leadership. DMDC exploits its centralized collection of manpower and personnel data to support Department-wide tracking, analyses, research, studies, and a wide variety of reporting requirements and operational programs. DMDC not only supports the execution, modification and maintenance of DoD and Congressionally mandated programs for personnel and medical benefits, readiness, and

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

force protection, but also implements new initiatives, which are highly useful extensions of existing systems. DMDC programs improve the effectiveness, efficiency, and productivity of personnel operations throughout DoD.

## **2.0. OBJECTIVES**

The contractor shall provide sustainment, upgrade, and system enhancement activities to include change management, problem management, performance management and capacity management as specified in this PWS. The contractor's activity is of a support nature only and shall not act as an agent of the Government at any time. Specific activities include the contractor supporting the sustainment and maintenance of the DCII and iIRR applications; application testing and deployment to include analysis or system performance; and supporting the development of DCII and iIRR projects. Contractor shall perform full life-cycle system management processes to build, sustain, and enhance DMDC technology and applications.

## **3.0 SCOPE OF WORK**

The Contractor is required to comply with all applicable laws, policies, procedures, and apply federal Government best practices. The Contractor will ensure all Information Technology projects, applications, systems, programs, or other areas of support provided hereunder comply with, adhere to and are guided by the standard program inception, elaboration, construction, and maintenance application life cycle methodology (see DoD Architecture Framework (DoDAF) version 2.0, Volume 1, refer to "4.7 Addressing Security Issues in DoDAF-Conformant Architecture Development," which will also point the contractor to Volume 2, Appendix A; see <<http://cio-nii.defense.gov/sites/dodaf20/>>).

## **4.0 TASK REQUIREMENTS**

The contractor shall provide skilled personnel capable of providing the full spectrum of sustainment and operational support for the DCII and iIRR application throughout the period of performance of this task order. The contractor shall perform sustainment activities of change management, problem management, performance management, capacity management and perform sustainment activities.

The contractor shall maintain required operational capability that includes supporting technology refresh, technology insertion and technical obsolescence risk management. The contractor shall perform comparative analyses of system health, provide analyses of solutions, and recommend solutions such as technology refresh.

The contractor shall sustain and support the DCII and iIRR applications in production, failover/COOP, pre-production, and test environments. As part of sustainment all software coding by the contractor shall be coded and initially tested in the contractor's environment. This

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

contractor's environment does not necessarily have to mirror the production environment. However, it is suggested that there be minimal differences to ensure minimal to no impact when deploying to pre-production, production, and failover/COOP sites. The contractor shall perform monitoring of system health and proactive reaction to signs of impending system outages.

The contractor shall sustain and support all applications in both production and test environments.

The contractor will maintain the necessary hardware and software in the contractor's environment to produce and/or test any code required to maintain the DCII and iIRR applications within the performance specifications of this PWS until the system has been fully transitioned into DMDC's environment. See Appendix G (Global Environment) for detailed information for the current DCII and iIRR production environment.

**4.1 Task 1 – Sustainment and Operational Support of DCII & iIRR**

The contractor shall provide ongoing support for applications covered under this task order within the production environment, and shall be responsible for ensuring the applications continue to function at the efficiency and capability levels intended as detailed in Appendices B (Guidelines and Parameters for Resolving System Problems), and C (System Outage Notification Procedures). ~~The contractor shall detect all outages or issues that adversely affect the performance of the system and take steps to remediate the problem.~~ The contractor shall notify all appropriate personnel so that the users can be promptly notified of system issues. The contractor shall modify the applications covered under this task order in accordance with Change Requests (CRs) and Problem Reports (PRs) approved by the DMDC Technical Point of Contact (TPoC). ~~Based on historical data, the Government anticipates 25 CRs/PRs per year.~~ This task shall include reverse engineering existing software to extract current business rules and supporting DMDC in the documentation of interface control documents. The contractor shall provide data extracts ad-hoc reports and maintain data accuracy.

The contractor shall assist in identifying and resolving application system problems, and recommend and coordinate hardware and software upgrades. The contractor shall adhere to requirements detailed in Appendices B and C. ~~The contractor shall utilize system monitoring techniques which will result in a proactive approach to identifying recurring problems, reporting to the Government those problems, and recommending solutions to mitigate recurring problems of the same nature.~~

The DCII production systems are located at the DMDC in Seaside, CA and in DMDC/HP Auburn Hills Service Management Center, Auburn Hills, MI.. The iIRR primary production system is located at DMDC in Seaside, CA.

The deliverables (electronic and hard copy): Completed schedule for delivery of testing of CRs/PRs in pre-production environment to be delivered 15 days prior to test start date.

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

**4.2 Task 2 – Application Failover/COOP System Support**

The contractor shall be responsible for the DCII failover/COOP system located at the DSS facility in Alexandria, VA. As part of Transition I, the DCII failover system will deploy to the Auburn Hills Service Management Center.

There is currently no failover system for iIRR. However, a future failover system will be located in the Auburn Hills Service Management Center upon completion of Transition Phase III.

DMDC and DSS will maintain the control of their respective parts of the networks until completion of Transition I and Transition III. Then, DMDC will have the sole control of the networks and systems. The task also requires failover planning and testing, both initial and on a regular basis.

Deliverables (electronic and hard copy) shall be the following:

Annually conduct a successful failover test (system switch over preferably scheduled over a weekend), run production for at least a period of one week from the failover production site, and then return back to the primary production site without loss or corruption of data and degradation of service.

- Disaster Recovery Test Plan

**4.3 Task 3 – New DCII System Stand-up Support (Transition Phase I)**

DMDC anticipates the need to stand up the DCII system on new hardware in the DMDC PSA enclave. The system will include: primary production system, located in Seaside, CA; secondary/COOP system, located in Auburn Hills, MI; and pre-production system, located in Seaside, CA.

Contractor shall deploy, configure, and fine-tune all components of the DCII application in new DMDC infrastructure.

Contractor shall plan and execute data migration from the old infrastructure to the new infrastructure without any loss or corruption of data and degradation of service.

The Contractor shall be responsible for sustainment tasks including but not limited to defect fixes, defect tracking, delivery of fixes, application code modifications to support hardware, configuration, and/or network changes, and design documentation.

This task includes migration from DSS to DMDC internal processes, which include: source code check-in; CM processes; Vulnerability Management, and the use of DMDC tools applicable to tasks in this PWS. For DMDC processes, use the following as reference guides Appendix D (DMDC Application Development Process) and Appendix E (DMDC PSA Interim Quality Assurance Requirements and Processes).

***This task shall be completed by May 31, 2011.***

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

**Deliverables:**

- Fully operational DCII application in production, failover/COOP, and pre-production environments in DMDC's infrastructure
- Disaster Recover Test Plan
- Backup and Recovery Procedure

**4.4 Task 4 -- New DCII System Stand-up Support (Transition Phase II)**

DMDC anticipates the need to stand up the DCII system on new hardware in the DMDC standard production enclave. The system will include: primary production system, located in Seaside, CA; secondary/COOP system, located in Auburn Hills, MI; and pre-production system, located in Seaside, CA.

The Contractor shall integrate all components of the DCII application from the DMDC PSA Enclave into the standard DMDC operational environment. The Contractor shall ensure that the system is built in accordance with DMDC policies and matches DMDC's system environment.

The Contractor shall be responsible for sustainment tasks including defect fixes, defect tracking, delivery of fixes, application code modifications to support hardware, configuration, and/or network changes, and design documentation.

The contractor shall provide support for the preparation, planning, and execution of migration of the supported applications from the DMDC PSA enclave into the DMDC standard production environment without any loss or corruption of data and degradation of service.

This task includes full migration from the DMDC PSA Enclave to DMDC internal processes, which shall include source code check-in; CM processes; Vulnerability Management, and the use of DMDC tools applicable to tasks in this PWS. For DMDC software processes and environment please use the following reference guides: Appendix D (DMDC Application Development Process) and Appendix G (DMDC Environment).

***This task shall be completed within 60 days from commencement.***

**Deliverables:**

- Fully operational DCII application in production, failover/COOP, and pre-production environments in DMDC's environment
- Disaster Recover Test Plan
- Backup and Recovery Procedure

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

**4.5 Task 5 - New iIRR System Stand-up Support (Transition Phase III)**

The Contractor shall integrate into the standard DMDC operational environment all components of the iIRR application from the DMDC, Boyers. The Contractor shall ensure that the system is built in accordance with DMDC policies and matches DMDC's system environment. This system will include: primary production system, located in Seaside, CA; secondary/COOP system, located in Auburn Hills, MI; and pre-production system, located in Seaside, CA.

The Contractor shall be responsible for sustainment tasks including defect fixes, defect tracking, delivery of fixes, application code modifications to support hardware, configuration, and/or network changes, and design documentation.

The contractor shall provide support for the preparation, planning, and execution of migration of the supported applications from the DMDC Boyers into the DMDC standard production environment without any loss or corruption of data and degradation of service. This task includes full migration from the DMDC Boyers to DMDC internal processes, which includes: source code check-in, CM processes, Vulnerability Management, and the use of DMDC tools applicable to tasks in this PWS.

For DMDC software processes and environment please use the following as reference guides: DCII and iIRR Global Environments (Appendix G), DMDC Application Development Process (Appendix E), and DMDC Environment (Appendix G).

***This task shall be completed within 60 days from commencement.***

Deliverables:

- Fully operational iIRR application in production, failover/COOP, and pre-production environments in DMDC's environment
- Disaster Recover Test Plan
- Backup and Recovery Procedure

**4.6 Task 6 -- Functional/Technical/Subject Matter Experts**

Contractor shall provide technical expertise and consultation support. The Contractor shall provide functional and technical expertise appropriate to support Government management. The contractor will support application/system configuration experience during the stand up of new systems (i.e., systems other than DCII and iIRR) in the DMDC enclave; migration of DCII and iIRR system from one DMDC enclave into another; or resolving technical issues with other PSA systems and/or interfaces between DMDC systems and non-PSA systems which involve configuration or technical information specific to the application(s) supported by the contractor. The Government anticipates up to 400 hours of support annually.

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

**4.7 Task 7 – Configuration Management (CM) Support**

This functional area consists of applying engineering and analytical disciplines to identify, document, and verify the functional, performance, and physical characteristics of systems, to control changes and nonconformance, and to track actual configurations of systems and platforms.

The contractor shall perform Configuration Management (CM) activities of configuration status accounting, configuration baseline management, creating and maintaining a configuration management library system to control the release of products and manage their history, and administering a change management procedure and tool to track all change requests (CRs) or problem reports (PRs) to the baseline as well as all issues (problem reports). The contractor shall respond to documents delivered with the software release. Update and re-deliver documents if not approved.

The contractor shall provide a Configuration Management (CM) Plan that follows industry standards and applies to the hardware, software (whether acquired or developed), and documentation developed, maintained, or operated by the contractor or Enterprise CM. The contractor shall follow the accepted and practiced Enterprise CM process in conjunction with DMDC internal and external procedures, plans, and policies.

The contractor shall inform, coordinate, and document all modifications to existing and developing system(s) under the DMDC's purview through the DMDC CM group. The contractor shall provide all baseline system documentation that includes system designs, build procedures, requirements documents test procedures, problem reports, software code, and system knowledge base and deliver to the Government upon final Government acceptance. The contractor shall coordinate with the DMDC CM group on all change management activities that affect the PSA systems and inform the DMDC CM group of internal changes that have potential impact to the PSA core services. The contractor shall provide technical support to DMDC CM on all aspects of project(s) deliverables.

The deliverables (electronic and hard copy) shall be the following:

- Configuration Management Plan to be delivered within 60 days of award
- Baseline documentation (designs, build procedures, requirements document, test procedures, problem reports, software code, knowledge base, etc.) after final acceptance

**4.8 Task 8 -- Quality Assurance**

The contractor shall develop, implement, and maintain a Software Quality Plan (SQP) to include resources required, schedules, tasks to be performed, procedures and tools to be used, records to be provided, the methodology of identifying and implementing process improvements in the software maintenance processes and related management areas, and the contractor's software

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

quality organization and interfaces. The Software Quality Plan will describe how the contractor's overall software quality program will be applied.

The contractor shall perform detailed reviews, walkthroughs, requirement traceability analyses, and defined verification and validation processes that occur during the course of software maintenance to ensure that requirements are traceable, consistent, complete, and testable. The contractor shall ensure the software correctly reflects the documented requirements. The contractor shall conduct, report on, and/or participate in formal reviews, informal reviews, inspections, peer reviews, tests, and evaluations for determining whether the code meets operational and security requirements. It is anticipated that this effort will require full-time support for an expert in each of the technologies used for DCII and iIRR.

The contractor shall ensure that quality assurance requirements are enforced for all aspects of a software revision process.

The contractor shall collect and analyze software quality metrics that include traceability, completeness, consistency, accuracy, simplicity, and modularity. The metrics are directly related to the non-functional requirements specified for the software.

The deliverables (electronic and hard copy) shall be the following:

- Software Quality Plan – initial, 10 days after task start date

Software Quality Plan – updated, with each release to be delivered 15 days prior to release testing in the pre-production environment.

#### **4.9 Task 9 -- Testing Support**

All software releases shall be developed and tested in the contractor's environment. Upon completion of the contractor's initial testing and quality assurance testing, all software coding will be tested in the Government's pre-production environment to ensure proper validation of enterprise systems and applications prior to deployment into the production environment. The contractor shall be responsible for fixing errors identified during the tests, to include tests in the Government's pre-production environment.

The contractor shall be responsible for creating and submitting for approval the Functional Test Guide. The Functional Test Guide includes system, stress, integration/interface and functional testing. The contractor shall conduct thorough tests to ensure that optimum performance is maintained. The contractor shall conduct functional testing of interfaces and application changes, as defined in the Functional Test Plan, prior to releasing the software for testing in the Government's pre-production environment. The contractor shall ensure that the most up-to-date application and database iterations are available for installation in the pre-production environment. The contractor shall provide the DMDC Quality Assurance team with a complete set of pertinent requirements and change control documentation so that the DMDC QA team can develop its own test scenarios, test and evaluation plans, and test analysis reports.

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

Once testing is accepted by the Government, the contractor shall deploy all new application releases to the Government's pre-production environment.

The deliverables (electronic and hard copy) shall be the following:

Functional Test Guide to be updated with each release and delivered 15 days prior to the scheduled test start date

**4.10 Task 10 -- User Acceptance Testing (UAT) for iIRR**

The Contractor shall be responsible for developing, reviewing, submitting and coordinating all necessary approvals of the User Acceptance Test Plan for selected software development projects for iIRR. UAT will include methodology, schedule and evaluation criteria used by the Contractor, in conducting the testing as well as making a deployment recommendation to the DMDC Technical Point of Contact (TPoC). The Contractor will work with the deployment team to conduct the testing and compile the results thereof. Based on the successful completion of Government Acceptance Testing and the DMDC Program Manager's decision, the application will be promoted to production. The UAT for iIRR will be performed at DMDC Boyers facility. The Government anticipates no more than 1 major release, which would result in 1 UAT per year.

The deliverables (electronic and hard copy) shall be the following:

- User Acceptance Test Plan

**4.11 Task 11 (Optional) -- Information Assurance/Computer Network Defense (IA/CND)**

The contractor shall support obtaining accreditation of the applications under this task order via certification testing of its respective element(s). This task will consist of process support, analysis support, coordination support, security certification test support, and security documentation support.

The contractor shall assist with system tests, e.g., stress, C&A, as described by Department of Defense Instruction (DoDI) 8510.10 and interface with other contractors/vendors, which support operation of the system, tests in the Government's pre-production environment, Government Acceptance Testing (GAT), and interface with other contractors/vendors that support the operation of the system. Certification testing consists of initial testing, monthly scans (for tools, see Attachment DX), annual compliance testing, and tri-annual recertification; each having remediation as a part of the event. In addition, there may be releases of software by the vendor that generate certification-testing engagements.

Process Support. The contractor shall assist the Government in the implementation of the Defense Information Assurance Certification and Accreditation Process (DIACAP). The contractor shall recommend process tailoring as provided for in the DIACAP, participate in process activities, and document the results of those activities.

The deliverables (electronic and hard copy) shall be the following:

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

- DIACAP Technical Report (monthly)

Analysis Support. The contractor shall test the adequacy of the required protective features of the DMDC assets located in the contractor's facility on a monthly basis using the Government-approved testing tools (for tools, see Appendix I (IA Scan Tools)) and provide the results to the Information Assurance Officer (IAO) no later than (NLT) the 28th day of each month. For detected vulnerabilities that could preclude/alter the status of the accreditation, the contractor shall implement human procedures, software configuration parameters, system changes, or combinations thereof to mitigate the risk associated with each vulnerability.

In accordance with the tools guidance found in Appendix I, the contractor shall test the adequacy of the required protective features using DISA tools such as Security Technical Implantation Guide (STIG), Security Readiness Reviews (SRRs) or checklist on a reoccurring basis using the appropriate tool (or other tool as defined by the Government). The contractor shall provide the results to the Information Assurance Officer (IAO) no later than (NLT) the 10 days after execution of the tool. For detected vulnerabilities that could preclude/alter the status of the accreditation, the contractor shall implement human procedures, software configuration parameters, system changes, or combinations thereof to mitigate the risk associated with each vulnerability.

Checklists exist for most technologies, but SRR Scripts only exists for some. For DMDC assets, UNIX, Apache Web Server, Windows Gold Disk, and MS SQLServer automated scanners are available. All other technologies require manual reviews. When the SRR scripts are available or the Gold Disk could be used, properly named original output files and the reports must be submitted after a successful review process. When an automated tool is not available, a manual review must be done using the applicable checklists. The results from the manual reviews must be reported using the included form or checklist itself. Below are the timelines for vulnerability remediation (periods may be overridden by direction of the Government and communicated via a Plan of Action and Milestones (POA&M) :

DoD SEVERITY	NIST SEVERITY	DAYS FOR COMPLIANCE/APPROVED MITIGATION
CAT I	HIGH	Immediate – 25 Days
CAT II	MEDIUM	60 Days
CAT III	LOW	180 Days
CAT IV	INFORMATIONAL	1000 Days

**Table 1 Compliance Timelines for Vulnerability Remediation**

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

The deliverables (electronic and hard copy) shall be the following:

- Monthly Vulnerability Scanning Results to include:
  - Category
  - Vulnerability ID
  - Short Description
  - Server Name
  - Instance name (if applicable)
  - Status (Open, Not a Finding, Not Applicable, Not Reviewed)
  - Comments
  - Recommendations
- The results from the manual reviews must be reported using the included form or checklist itself
- Properly named, original output files

c. Coordination Support. The contractor shall coordinate with or participate in monthly meetings with the Information Assurance Manager (IAM) and IAO to keep them informed on system security matters, address specific security issues, and obtain guidance. The contractor shall coordinate or participate in monthly meetings with other organizations as directed by the Government.

d. Security Certification Test Support. In addition to the testing performed for Analysis Support, the contractor shall support the DMDC Information Systems Security Group (DISSG). This support includes pre-test preparations, participation in the tests, assistance with the interpretation of the results, and remediation of vulnerabilities. The tools utilized for this function are noted in Attachment D.

e. Security Documentation Support. The contractor shall document the results of DIACAP process activities and contractor technical or coordination activity. The contractor shall prepare/update the 1) Concept of Operations, 2) System Rules of Behavior, and 3) System Security Plan (SSP) portions of the System Security Authorization Agreement (SSAA). All documents shall be prepared and/or maintained in accordance with the cited attachments.

The deliverables (electronic and hard copy) shall be the following:

- Concept of Operations (template is available as IEEE 1361-1998)
- System Rules of Behavior
- System Security Plan

f. Joint Task Force-Global Network Operations (JTF-GNO) Direction. The contractor shall provide Information Assurance/Computer Network Defense (IA/CND) services in accordance

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

with the requirements promulgated by JTF-GNO. This task will consist of Security Operational Services and Security Planning Services.

g. Security Operational Services. The contractor shall provide security services for protection of the Information Systems, Information System Domains (Communities of Interest), and Information Content (at rest, in use, and in transit) in accordance with DoD Information Assurance policies and procedures. These security services shall be provided to protect all sensitive information. These operational security services shall be fully integrated with JTF-GNO mandates to ensure confidentiality, integrity, availability, authenticity, and non-repudiation requirements. The contractor shall implement the necessary IA/CND mechanisms to provide these security services, and shall conduct vulnerability assessments to validate that the necessary controls are in place. As part of implementing these security services, the contractor shall be responsible for implementing Government directed IA/CND direction such as INFOCONs (information operations conditions) and incident reporting (e.g., system anomalies, outages, etc.). Implementation of IA/CND mandates, to include JTF-GNO Communications Tasking Orders (CTOs), Warning Orders (WARNORD), Operational Directive Messages (ODM), Information Special Outage Report (INFOSPOT), Situational Awareness Report (SITREP), and Fragmentary Order (FRAGO) shall be accomplished within Government specified timeframes. As part of these security services, the contractor shall make available near-real time data feeds, or provide real-time data feeds where available, to support Government oversight detailing the security operational functions.

The deliverables (electronic and hard copy) shall be the following:

- IA/CND Technical Report to be produced monthly, negative reporting is required
- Incident Report to be produced monthly, negative reporting is required.

h. Security Planning Services. The contractor shall provide strategic security services to enhance the confidentiality, integrity, availability, authenticity, and non-repudiation requirements. The contractor shall support the use of the following mechanisms of encryption, access control, user identification and authentication, malicious content detection, audit, and physical and environmental control. The contractor shall make available information feeds to support Government oversight, maintain accessible historical data, and provide summary management reports that detail the security planning functions. The contractor shall propose updated and/or revised architecture and/or configuration change designs to accommodate changing requirements, emerging technology, and results of vulnerability assessments for Government review and approval.

The deliverables (electronic and hard copy) shall be the following:

- Security Planning Functional Technical Report to be produced bi-annually

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

The contractor shall meet DoD and DMDC security requirements. Refer to Appendix J (DMDC Information Assurance Policy).

**4.12 Task 12 (Optional) – Vulnerability Management**

The DMDC anticipates approximately 20 Information Assurance Vulnerability Management (IAVM) actions monthly. The IAVM program includes three types of vulnerability notifications:

- An **Information Assurance Vulnerability Alert (IAVA)** addresses vulnerabilities resulting in immediate and potentially severe threats to DOD systems and information. Corrective action is of the highest priority due to the severity of the vulnerability risk.
- An **Information Assurance Vulnerability Bulletin (IAVB)** addresses new vulnerabilities that do not pose an immediate risk to DMDC systems, but are significant enough that noncompliance with the corrective action could escalate the risk.
- A **Technical Advisory (IATA)** addresses new vulnerabilities that are generally categorized as low risks to DOD systems.

The DMDC IAVM program directs that all **IAVA/IAVB/IATA** notices are effective **immediately**. The DMDC IAVM program applies to all devices on all DMDC owned, controlled, or contracted information system or network. All DMDC owned, controlled, or contracted systems will be considered non-compliant and at risk as soon as an IAVM action is issued and will remain non-compliant until all systems are patched.

The compliance timelines for IAVAs are in effect upon issuance, and are mandatory as directed by the CYBERCOM. The timeline for compliance on IAVBs and TAs vulnerabilities are determined by the assigned severity for the vulnerability coupled with the compliance timelines established by DISA.

Severity codes (“STIG Finding Severity”) are documented in the IAVM notices published on the CYBERCOM Web Page. DISA, as a C/S/A, has determined the following compliance requirements based on severity (periods may be overridden by direction of the Government and communicated via a Plan of Action and Milestones (POA&M)). See Table (below) for guidance:

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

<b>DoD SEVERITY</b>	<b>NIST SEVERITY</b>	<b>DAYS FOR COMPLIANCE/APPROVED MITIGATION</b>
<b>CAT I</b>	<b>HIGH</b>	<b>Immediate—25 Days</b>
<b>CAT II</b>	<b>MEDIUM</b>	<b>60 Days</b>
<b>CAT III</b>	<b>LOW</b>	<b>180 Days</b>
<b>CAT IV</b>	<b>INFORMATIONAL</b>	<b>1000 Days</b>

**Table: Compliance Timelines for IAVM Actions**

The contractor must take immediate action to assess the impacts of each vulnerability, develop patching plans, and begin gathering data for the new “First Report” requirement. The patch plan should consider Legacy Systems, Programs of Record, and other systems that may not be patched by the Plan of Action and Milestones (POA&M) report date. DMDC Technical Point of Contact (TPoC) must begin evaluating these systems for possible POA&M actions as soon as possible.

Testing must be conducted to ensure IAVM actions will not impair system operations. IAVM compliance will be ensured through 1) the normal Certification and Accreditation (C&A) process (DIACAP), and 2) monthly scanning of the systems using tools outlined in Table 3-2. The results of these scans will be sent to the Information Assurance Officer (IAO).

This task shall be finished upon the completion of the Transition Phase II for DCII and Transition Phase III for iIRR outlined in this PWS.

#### **4.13 — Task 13 — System Security Engineering (SSE) Support**

The contractor shall provide SSE support in design, risk assessment, and systems testing. This task will consist of SSE Requirements, Vulnerability Analyses, System Security Concept of Operation (SSCO), Tailored Security Plans, System Security Assessments, and Self Evaluation.

a. SSE Requirements. The contractor shall assist in developing program specific SSE requirements. The contractor shall review conceptual studies, program reports, system data and other pertinent source documentation which might aid in establishing basic system security requirements. These requirements will be documented in the systems specifications.

The deliverables (electronic and hard copy) shall be the following:

- Changes to Systems Specifications as required by system releases

b. Vulnerability Analyses. The contractor shall review program threats and conduct vulnerability analyses to define security functional requirements for effectively securing systems against overt

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

and covert attack. The contractor shall provide recommendations for the integration of security countermeasures and other corrective actions.

The deliverables (electronic and hard copy) shall be the following:

- Vulnerability Analysis Technical Report monthly with negative reports required

e. System Security Concept of Operation (SSCO). The contractor shall develop a System Security Concept of Operation (SSCO) based on the threat definition, vulnerability analyses, and existing security systems and measures. The SSCO shall describe mission tasks, operational system specifications, security resource requirements, threat environment, protection of Critical Program Information (CPI), employment issues, and manpower costs.

The deliverables (electronic and hard copy) shall be the following:

- SSCO initial report due within 180 days of award
- SSCO quarterly with negative reports required

d. Tailored Security Plans. The contractor shall plan, design, review, analyze and report on tailored security plans for the protection of systems during the test and evaluation phase and make recommendations for changes to security test procedures.

The deliverables (electronic and hard copy) shall be the following:

- Tailored Security Plan monthly with negative reporting required

e. System Security Assessments. The contractor shall assist in conducting system security assessments to assure the proper front end emphasis on System Security Management.

The deliverables (electronic and hard copy) shall be the following:

- System Security Assessment to be completed with each release analysis

f. Self Evaluation. The contractor shall continuously analyze the adequacy of the contractor's system security planning and physical security standards and report on discrete areas of concern.

The deliverables (electronic and hard copy) shall be the following:

- Self Evaluation Technical Report monthly with negative reporting required

This task shall be finished upon the completion of the Transition II for DCII and Transition III for iIRR outlined in this PWS.

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

**4.14 Task 14 -- Database Administration**

The contractor shall provide database administration services that shall accomplish modifications to any system or production application database, to include pre production database, covered under this task order, while maintaining continuity of the data. The contractor shall perform schema changes and conversion of the production database during application upgrades and new version releases. The contractor shall also maintain database replication between all backup site locations and all server replicates. In addition, the contractor shall support, maintain, and keep the development, test, and pre production environment consistent with current application upgrades and new version releases, while providing database refreshment of all database instances.

**4.15 Task 15 -- Data Analysis and Cleansing**

The contractor shall ensure data integrity; analyze data errors causing problems in the legacy applications or other errors that exist in the aforementioned programs areas. The contractor shall ensure that problems are resolved. If the source of the problem is from a data interface, the contractor shall notify the data source, and provide advice to the data source on how the problem may be solved.

**4.16 Task 16 -- Customer and Field Support**

The contractor shall support customer requests for the following activities:

- a. Develop ad hoc reports. The Government anticipates 84 reports yearly for both systems combined.
- b. Assist Program Managers with problem reports as they relate to the applications
- c. Provide review, evaluation, advice, and/or guidance on products or deliverables relating to the applications
- d. The contractor shall provide assistance with Help Desk tickets. The Government anticipates 180 tickets annually for both systems combined.

**5.0 PERIOD OF PERFORMANCE**

The base period of performance for this order shall be a one (1) year from the date of award with one (1) one-year option period that will be exercised at the discretion of the Government.

**6.0 PLACE OF PERFORMANCE** The primary work location will be at the contractors location(s) with travel to the following DMDC locations: DMDC Seaside - 400 Gigling Road, Seaside, CA; DMDC Arlington - 1600 Wilson Blvd, Arlington, VA; DMDC Mark Center - 4800 Mark Center Dr, Alexandria, VA; DMDC Boyers - 1137 Branchton Road, Boyers, PA ; HP Center - Auburn Hills, MI.

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

## **7.0 DELIVERABLES AND REPORTS**

**7.1 The contractor shall provide the following deliverables and reports: (See Appendix N)**

### **7.1.1 Problem Reports**

The contractor shall bring problems or potential problems affecting performance to the attention of the COR and CO as soon as possible. Verbal reports shall be followed up with written reports when directed by the COR or CO.

### **7.1.2 Senior Management Review (SMR) Reports (Appendix K)**

An SMR report shall be submitted every 15<sup>th</sup> of each month. The monthly SMR report shall summarize the following information:

- Financial Review/Expenses,
- accomplishments during the period,
- problems met or anticipated,
- activities anticipated during the next reporting period, and
- utilization of personnel.

See Appendix C for an acceptable sample format. These reports shall be submitted to the Contracting Officer's Representative (COR) by e-mail.

Each monthly SMR report shall be submitted by the 15th business day of the month following the period reported upon.

### **7.1.3 Funding Notification**

The contractor shall notify the CO, by written memorandum, concerning issues that may lead to any funding shortfalls, risk situations, or adjustments stemming from Government direction or prioritization of work that is outside of the scope of this PWS.

### **7.1.4 Quality Control Plan**

The Appendix L (Quality Control Plan (QCP)) is the contractor's internal plan to insure delivery of quality products and services under the terms of the contract. The QCP shall detail the contractor's internal controls for services under this contract and should have a direct relationship to the proposed terms of the Performance Requirements Summary (PRS). See Appendix M. The completed QCP shall be delivered 45 days after award.

## **7.2 Delivery, Inspection, and Acceptance Instructions**

The contractor shall deliver all end items specified in this PWS / Deliverable table electronically (with contractor's letterhead - cover letter) to the COR, TPOC, and CO unless otherwise specified. The Government will review any 'draft' documents and notify the contractor of

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

approval or recommended changes to be made in the 'final' version within 30 days. 'Final' deliverables are then due within 10 working days after receipt of any Government comments on the draft unless otherwise specified by the Government

## **8.0 CONTRACTOR PERSONNEL**

### **8.1 Key Personnel Requirements**

The following labor categories are considered key personnel by the Government: Program Manager, Database Administrator/Manager, and Senior Test Engineer. Qualifications for all key personnel are to be proposed by the Contractor and resumes are to be provided. When accepted, these qualifications shall form the minimum requirements for the key personnel positions. Key personnel may not be removed from the task without express approval of the COR. Staff may be proposed to replace key personnel and should be of equal or greater qualifications. During task order performance, resumes should be submitted for proposed replacements at least 10 working days prior to the time the personnel change is expected to occur and must be accepted by the Government.

### **8.2 Identification of Contractor Employees**

All contract personnel attending meetings, answering Government telephones, and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. Electronic mail signature blocks shall identify contractor/company affiliation. They must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed. Contractor personnel occupying collocated space in a Government facility shall identify their workspace with their name and company/contractor affiliation.

### **8.3 Organizational Conflict of Interest**

Contractor and subcontractor personnel performing work under this contract may receive, have access to, or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.), or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The Contractor's mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may effect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

#### **8.4 Unauthorized Disclosure**

The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases. If either the Government or the Contractor discovers new or unanticipated threats or hazards, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

#### **9.0 SECURITY**

DoD 5200.2-R, DoD Personnel Security Program, assigns DoD contractor personnel who perform work on IT systems to one of three ADP position categories (ADP-I, ADP-II, ADP-III) that equate to Critical Sensitive, Non-Critical Sensitive, and Non-Critical, respectively. DoDI 8500.2, Information Assurance Implementation renamed the ADP position categories as IT Level I (IT-I) (Privileged), IT-II (Limited Privileged), and IT-III (Non-Privileged), respectively. The term IT is synonymous with the older term ADP.

Any contractor employees who work in support of this order that have access to the DoD sensitive data must comply with the National Agency Check with Inquiries (NACI) investigative process for IT-II access in accordance with procedures identified by the DMDC Information Systems Security Group (DISSG) responsible for oversight of all security at DMDC. Individuals proposed for positions on this order must be capable of being "vetted" to the IT level, as determined / specified by DMDC, in accordance with DoD Regulation 5200.1-R. Personnel who are charged with security as a duty should be professionally certified to the IT level-1 category as specified in 8570.01-M.

The contractor must implement non-disclosure statements to be signed by all of its employees with access to DMDC applications, Administrator passwords (such as for, but not limited to RAPIDS, DBIDS, DNVC, DCCIS, NTS, ETAS, etc.) to ensure that portion of the DoD PKI remains safeguarded. The contractor should refer to DoD Regulation 5200.2-R, Personnel Security Program for details.

While visiting Government facility, all contractor personnel shall wear Government-issued access badges with coloration that distinguishes contractors from Government employees and "contractor" designation clearly displayed on the badge.

#### **9.1 National Agency Check & Inquiries (NACI)**

Tasks (not related to classified systems/applications) described in this PWS or resultant Task order is Unclassified, unless otherwise specified. For Unclassified projects, the level of clearance, National Agency Check & Inquiries (NACI), or IT level of access required is

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

specified in DoD Regulation 5200.1-R. All personnel working on these tasks will be required to successfully complete / pass a NACI. Individuals proposed for positions must be capable of being qualified at the proposed the IT level in accordance with DoD Regulation 5200.1-R. If the task is identified as classified, then the appropriate security clearance level is required for personnel requiring access to the classified portions of the project(s).

**U.S. citizenship** is required for all personnel who have not submitted trustworthiness determination and/or security clearance prior to October 26, 2006. All documentation and cost for clearance processing shall be the responsibility of the contractor. No contractor employee shall commence work under this task order until the appropriate paperwork for trustworthiness determination and/ or security clearance has been granted.

## **9.2 Trustworthiness Determination and Security Clearances**

Work on this project may require that personnel have access to sensitive unclassified information. In the event the contractor is given access by the Government to sensitive Government data, the contractor hereby agrees to protect such data from unauthorized use or disclosure as long as such data remains sensitive. In order to protect this sensitive information the contractor shall comply with DoD Regulation 5200.1-R, Information Security Program and DoD Regulation 5200.2-R, Personnel Security Program.

Some tasks on this order require employees assigned to work on those tasks to have a security clearance at a minimum of the SECRET level. This requirement is identified in the tasks, accordingly.

The contractor shall take reasonable care to deny access to unauthorized persons, maintain an established information security policy, and uphold procedures for safeguarding and controlling the protected information, so that it is exposed only to those who have a need to know the information and a duty to protect it. The duty to protect shall be established by a non-disclosure statement with the employee.

Additionally, as required personnel will have access to system administrator accounts and passwords, the contractor shall safeguard this information and shall not share this information, without the express permission of the Government Technical Point of Contact (TPOC). The contractor personnel issued CACs will be required to sign a DD Form 2841, "Department of Defense (DoD) Public Key Infrastructure (PKI) Certificate of Acceptance and Acknowledgement of Responsibilities" and shall adhere to these responsibilities.

Contractors are required to complete annual Security Awareness training and other security related training provided by the DMDC to ensure users understand all DMDC and DoD protocols.

## **9.3 IT Security Compliance**

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

The Contractor shall abide by DoD and DMDC security policies and models for system architecture and technology. The contractor shall meet DoD and DMDC security requirements.

**9.4 Privacy Act**

Work on this project may require that personnel have access to Privacy Information. Personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations.

**9.5 Protection of Personally Identifiable Information (PII)**

(a) To the extent that the work under this task order / agreement requires the contractor to have access to personally identifiable information about an individual (hereinafter referred to as “PII”), the contractor shall after receipt thereof, treat such PII as confidential and safeguard such information from unauthorized use and disclosure. The contractor agrees not to appropriate such PII for its own use or to disclose such information to third parties unless specifically authorized by the Government, in writing.

(b) The contractor agrees to allow access only to those employees who need the PII to perform services under this task order and agrees that PII will be used solely for the purpose of performing services under this task order. The contractor shall ensure that its employees will not discuss, divulge or disclose any such PII to any person or entity except those persons within the contractor’s organization directly concerned with the performance of the task order.

(c) Contractor shall administer a monitoring process to ensure compliance with the provisions of this clause. Any discrepancies or issues should be discussed immediately with the Contracting Officer Technical Representative (COTR) and corrective actions will be implemented immediately.

(d) The contractor shall report immediately to the DMDC CIO / Privacy Office and secondly to the COTR discovery of any Privacy breach. Protected PII is an individual’s first name or first initial and last name in combination with any one or more of the following data elements including, but not limited to: social security number; biometrics; date and place of birth; mother’s maiden name; criminal, medical and financial records; educational transcripts, etc.

(e) The Government may terminate this task order for default if contractor or an employee of the contractor fails to comply with the provisions of this clause. The Government may also exercise any other rights and remedies provided by law or this task order, including criminal and civil penalties.

(f) In accordance with the Privacy Act of 1974 Section (m) (1) contractors supporting a Government agency shall be considered to be an employee of that agency. As such all contractors will be required to take Privacy training, provided by the Government, upon hiring and annually. Additional specialized training may also be required.

(g) The Contractor shall include this section in all appropriate subcontracts.

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

(h) TS clearance area

**9.6 Physical Security**

The contractor shall be responsible for safeguarding all Government equipment, information and property provided for contractor use. At the close of each work period, Government facilities, equipment, and materials shall be secured.

**9.7 Government Facility Access**

For selected personnel at contract award and in coordination with Technical Point of Contact (TPoC), the contractor shall request and obtain Common Access Cards (CAC) for logical and/or physical access to Government resources. The Contracting Officer's Representative (COR) shall notify the contractor of any increased security requirements, if they occur, and the contractor shall submit adequate clearance packages within 10 calendar days of identification of increased security requirements.

**9.8 Personal Identity Verification of Contractor Personnel**

As prescribed in 4.1301, insert the following clause: Personal Identity Verification of Contractor Personnel (Jan 2006) (a) The Contractor shall comply with agency personal identity verification procedures identified in the contract that implement Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) guidance M-05-24, and Federal Information Processing Standards Publication (FIPS PUB) Number 201. (b) The Contractor shall insert this clause in all subcontracts when the subcontractor is required to have physical access to a federally-controlled facility or access to a Federal information system.

**10.0 OTHER PERFORMANCE REQUIREMENTS**

**10.1 Orientation Briefing**

Within two weeks of award, the Contractor shall conduct an orientation briefing for the Government. The Government does not want an elaborate orientation briefing nor does it expect the Contractor to expend significant resources in preparation for this briefing. The intent of the briefing is to initiate the communication process between the Government and Contractor by introducing key task participants and explaining their roles, reviewing communication ground rules, and assuring a common understanding of subtask requirements and objectives. The Orientation Briefing's place, date and time shall be mutually agreed upon by both parties within a week from the date of award. The completion of this briefing will result in the following:

- a) Introduction of both Contractor and Government personnel performing work under this Task Order.
- b) The Contractor will demonstrate confirmation of their understanding of the work to be accomplished under this PWS.

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

The Contractor shall provide two (2) hard copies of their proposal (technical and price) to the Government at the Orientation Briefing.

**10.2 Transition/Phase-In**

The Contractor shall assist in the transition of this contract to a successor contractor. The transition period shall consist of the final 30 calendar days of the contract. On the last calendar day of the transition, the successor will assume all responsibilities. The following shall apply only to a transition wherein the contractor is not the recipient of the successor award:

- The Contractor shall provide the successor with detailed briefings regarding the structure of the database tables and software required continuing maintenance and operation of systems developed under this contract.
- The Contractor shall transfer all project materials to the successor Contractor upon direction from the Contracting Officer and in a manner prescribed by the Government. Transfer shall be completed by the expiration date of the contract and shall include provision by the incumbent Contractor of accurate and complete data files and pertinent documentation.
- The Contractor shall transfer the source files and documentation for all software developed on this contract to the successor Contractor.
- Transfer shall be completed by the expiration date of the contract and shall include provision by the incumbent Contractor of accurate and complete source files and documentation for all software developed.
- For a contractor other than the incumbent provide a detailed plan and timetable for implementing the transition from the current facility to the proposed facility. The Contractor shall be responsible for the physical move of all inventories. The move shall be accomplished prior to the effective date of the contract.

**10.3 Hours of Operation**

The Contractor is responsible for conducting business between the hours of 8 a.m. to 5 p.m. Eastern Time, Monday thru Friday (except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings) however, the Contractor's Key Personnel should be reachable by phone within two hours in emergency situations. The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

the Government facility is not closed for the above reasons. When hiring personnel, the Contractor shall keep in mind that the stability and continuity of the workforce are essential.

#### **10.4 Government Holidays**

The following Government holidays are normally observed by Government personnel: New Years Day, Martin Luther King's Birthday, Presidential Inauguration Day (metropolitan DC area only), President's Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veteran's Day, Thanksgiving Day, Christmas Day, and any other day designated by Federal Statute, Executive Order, and/or Presidential Proclamation. Or any other kind of administrative leave such as acts of God (i.e. hurricanes, snow storms, tornadoes, etc) Presidential funerals or any other unexpected Government closures.

#### **10.5 Contractor Interfaces**

The Contractor and/or its subcontractors may be required as part of the performance of this effort to work with other Contractors working for the Government. Such other Contractors shall not direct this Contractor and/or their subcontractors in any manner. Also, this Contractor and/or their subcontractors shall not direct the work of other Contractors in any manner. The Government shall establish an initial contact between the Contractor and other Contractors and shall participate in an initial meeting. Any Contracting Officer's Representatives (COR) of other efforts shall be included in an initial meeting.

#### **10.6 Remote Access**

Contractor will use DMDC's remote access network infrastructure. The contractor will furnish:

- Stable, high-quality Internet Bandwidth
- Non-GFE workstations capable of installing and executing hardware and software necessary to use VPN remote access tools for network authentication and access control points. Non-GFE workstations shall include standard peripheral devices required for complete functionality (i.e., monitor, keyboard, mouse, etc). In addition, the contractor shall provide the following additional peripheral devices: Common Access Card (smartcard) compatible card reader and webcam.
- The contractor shall comply with all information technology security requirements. For Non-GFE workstations capable of access the DMDC network, the contractor shall maintain patch levels in compliance with the DoD's IAVA program; maintain antivirus updates; and, maintain DMDC mandated software configurations.
- The contractor shall, when security incidents are detected regardless of the source of the incident, promptly notify the DMDC help desk as well as immediately discontinuing the use of workstations. If malware is the source of the security incident, the contractor shall promptly eradicate the malware.
- Non-secure Telephone, facsimile, and voicemail capabilities.

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

The Government shall provide VPN remote access tools as GFE. Non-GFE workstations shall be capable of installing and executing the following software configurations (VPN access tools): Cisco VPN client; Microsoft Windows Terminal Service client; ActivClient 6 or newer; and Antivirus DoD approved vendor & version.

Remote access is controlled via a Common Access Card (CAC)-enabled to access Virtual Private Network (VPN). The contractor shall ensure that only those personnel having a compelling operational need will request such access and shall keep this number to the absolute minimum necessary to accomplish the mission. This access will be granted to personnel only via an approved System Access Request (SAR). Access will only be granted from the contractor's or DMDC's network. This subnet will conform to DoD Directive 8500.1, DoD Instruction 8500.2, and appropriate Security Technical Implementation Guides, including, but not limited to, Secure Remote Computing, Enclave Security, and Network Infrastructure. The subnet will require accreditation by the DMDC Designated Accrediting Authority (DAA) under the DoD Information Assurance Certification and Accreditation Process (DIACAP). The contractor shall assist with the implementation of the DIACAP on this subnet.

#### **11.0 TRAVEL**

Travel may be required at irregular intervals to the DMDC locations. The Contractor will be reimbursed for travel to provide support at a Government site or other site as may be specified and approved by the COR under this effort. All travel shall be approved, by the COR, prior to commencement of travel. The contractor shall be reimbursed for actual allowable, allocable, and reasonable travel costs, including local travel, incurred during performance of this effort in accordance with the Joint Travel Regulations (JTR) currently in effect on the date of travel.

#### **12.0 GOVERNMENT FURNISHED PROPERTY/INFORMATION**

The contractor should assume that the GFE currently being used for the ISFD/DCII/iIRR Sustainment Contract GS09K99BHD0010 will be provided for this contract on April 1, 2011. A list of the GFE is provided in Appendix P. The contractor should assume it will be responsible for providing all other resources including all personnel, equipment (such as developer workstations), supplies, facilities, transportation, tools, materials, supervision, and other items necessary to provide the non-personal services detailed herein at the contractor facility. The contractor's environment does not have to mirror the production, pre-production, and failover environments.

#### **13.0 ADMINISTRATIVE CONSIDERATIONS**

##### **13.1 Correspondence**

To promote timely and effective administration, correspondence shall be subject to the following procedures:

- a) Technical correspondence (where technical issues relating to compliance with the requirements herein) shall be addressed to the Contracting Officer's Representative

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

(COR) with an information copy to the Contracting Officer (CO) and the Contract Administrator (CA).

- b) All other correspondence, including invoices, (that which proposes or otherwise involves waivers, deviations or modifications to the requirements, terms or conditions of this PWS) shall be addressed to the Contracting Officer with an information copy to the COTR.

### **13.2 Points of Contact**

Contracting Officer Representative (COR) for this effort is as follows:

Craig Brugger  
4800 Mark Center Dr.  
Alexandria, VA 22350-0001  
Phone: (b) (6)  
Email: [craig.brugger@osd.pentagon.mil](mailto:craig.brugger@osd.pentagon.mil)

#### **Contracting Officer (KO)**

Eileen Flanigan  
GSA—Federal Acquisition Services, Region 3  
20 N. 8<sup>th</sup> Street, 10<sup>th</sup> Floor  
Philadelphia, PA 19107  
Phone: (b) (6)  
Email: [eileen.flanigan@gsa.gov](mailto:eileen.flanigan@gsa.gov)

#### **Contract Specialist**

Michelle Carney  
GSA—Federal Acquisition Services, Region 3  
20 N. 8<sup>th</sup> Street, 10<sup>th</sup> Floor  
Philadelphia, PA 19107  
Phone: (b) (6)  
Email: [charlotte.carney@gsa.gov](mailto:charlotte.carney@gsa.gov)

#### **Client Service Representative (PM/ITM)**

Michael Baumann  
GSA – Federal Acquisition Services, Region 3  
20 N. 8<sup>th</sup> Street, 10<sup>th</sup> Floor  
Philadelphia, PA 19107  
Phone: (b) (6)  
Email: [michael.baumann@gsa.gov](mailto:michael.baumann@gsa.gov)

**PERFORMANCE-BASED WORK STATEMENT**  
**Defense Central Index of Investigations (DCII)**  
**& Improved Investigative Records Repository (iIRR)**  
**Sustainment Support Services**  
**Revised March 1, 2012**

**13.3 Clauses (See Appendix O)**

**14.0 SECTION 508 COMPLIANCE REQUIREMENTS**

The contractor shall support the Government in its compliance with Section 508 through-out the development and implementation of the work to be performed. Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d) requires that when Federal agencies develop, procure, maintain, or use electronic information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who do not have disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities who are members of the public seeking information or services from the Federal Agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency. The Offer should review the following websites for additional 508 compliance information.

<http://www.section508.gov/index.cfm?FuseAction=Content&id=12>

<http://www.access-board.gov/508.htm>

<http://www.w3.org/WAI/Resources>